Nessus Vulnerability Scanning Project

Table of Contents

Project Overview

Purpose

This project demonstrates the complete workflow of using Nessus vulnerability scanner to identify, analyze, and remediate security vulnerabilities in a network environment using Kali Linux on Oracle VirtualBox.

Learning Objectives

- Understand vulnerability assessment fundamentals
- Install and configure Nessus Essentials
- Perform comprehensive vulnerability scans
- Analyze and prioritize security findings

- Develop remediation strategies
- Apply security best practices

Environment

- **Host OS**: Windows/macOS/Linux
- **Virtualization**: Oracle VirtualBox
- **Guest OS**: Kali Linux (Latest version)
- **Scanner**: Nessus Essentials (Free version)
- **Target**: Metasploitable 2/3 or other vulnerable VMs

What is Nessus?

Definition

Nessus is a comprehensive vulnerability assessment solution developed by Tenable that identifies security weaknesses, configuration issues, malware, and policy violations across networks, systems, and applications.

Key Features

- **60,000+ vulnerability checks**: Extensive plugin library
- **Configuration auditing**: CIS benchmarks, PCI-DSS compliance
- **Malware detection**: Identifies suspicious processes
- **Credentialed scanning**: Deep system analysis
- **Web application scanning**: OWASP Top 10 vulnerabilities
- **Cloud infrastructure scanning**: AWS, Azure, GCP support

How It Works

1. **Discovery Phase**: Identifies live hosts and open ports
2. **Vulnerability Detection**: Tests for known vulnerabilities
3. **Analysis**: Assigns severity ratings (Critical, High, Medium, Low, Info)
4. **Reporting**: Generates detailed reports with remediation guidance

Prerequisites

Hardware Requirements

- **RAM**: Minimum 4GB (8GB recommended)
- **Storage**: 20GB free space
- **CPU**: Dual-core processor (Quad-core recommended)
- **Network**: Active internet connection

Software Requirements

- Oracle VirtualBox (latest version)
- Kali Linux ISO (latest version)
- Target vulnerable VM (Metasploitable 2 recommended)

Knowledge Requirements

- Basic Linux command-line skills
- Understanding of networking concepts (IP, TCP/IP, ports)
- Familiarity with cybersecurity terminology

Installation Guide

Step 1: Download Nessus Essentials

1. Navigate to: https://www.tenable.com/products/nessus/nessus-essentials
2. Click **"Register for Nessus Essentials"**
3. Fill out the registration form with valid email
4. Select **"Nessus-#.##.#-debian6_amd64.deb"** for Kali Linux
5. Save the activation code sent to your email

Step 2: Install Nessus on Kali Linux

Open a terminal and execute the following commands:

bash

Update system packages

sudo apt update && sudo apt upgrade -y

Navigate to the Downloads directory

cd ~/Downloads

Install the Nessus package

sudo dpkg -i Nessus-*.deb

Start Nessus service

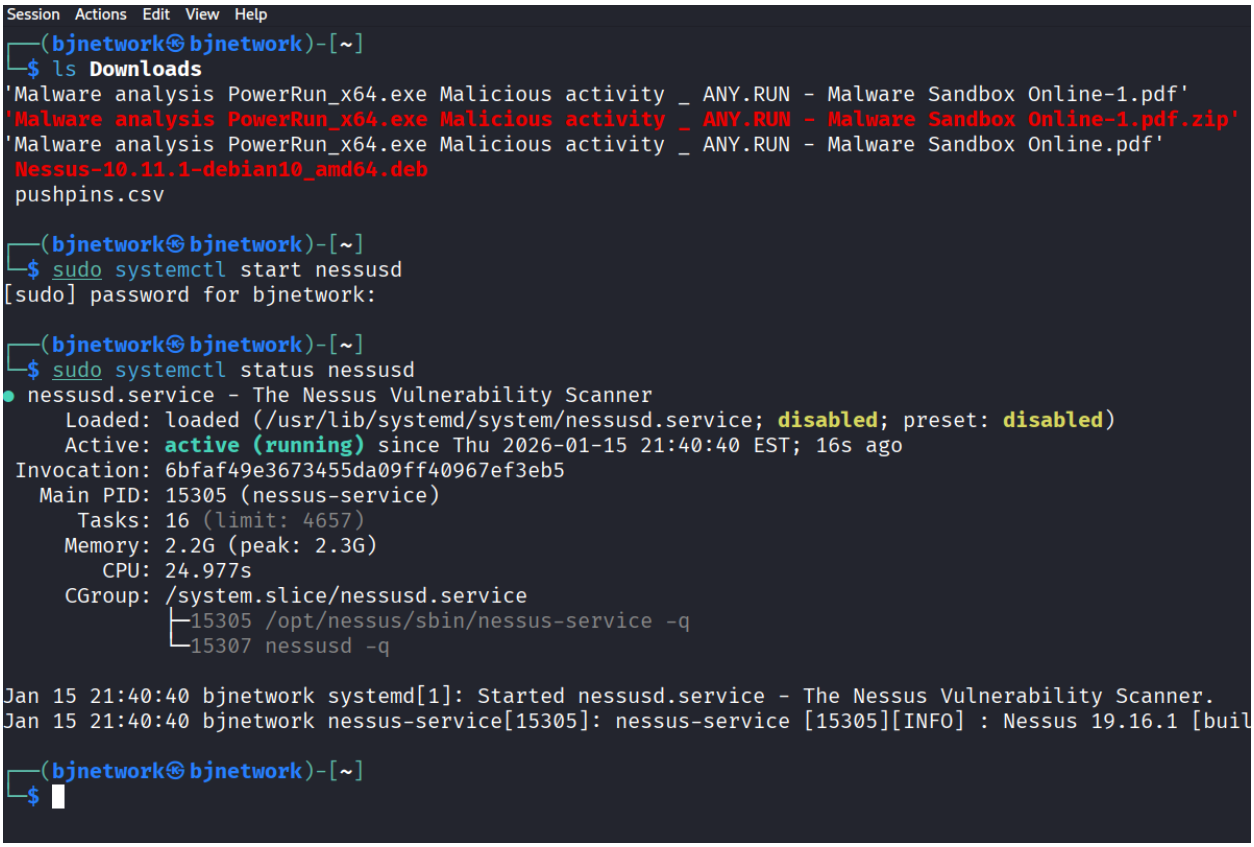
sudo systemctl start nessusd

Enable Nessus to start on boot

sudo systemctl enable nessusd

Check service status

sudo systemctl status nessusd



Step 3: Access Nessus Web Interface

bash

Nessus runs on port 8834

Open a web browser and navigate to:

https://localhost:8834

Initial Configuration

Step 1: Welcome and Setup

1. Click **"Nessus Essentials."**
2. Enter the activation code from your email
3. Create admin username and password (use strong credentials)
4. Click **"Continue."**

Step 2: Plugin Download

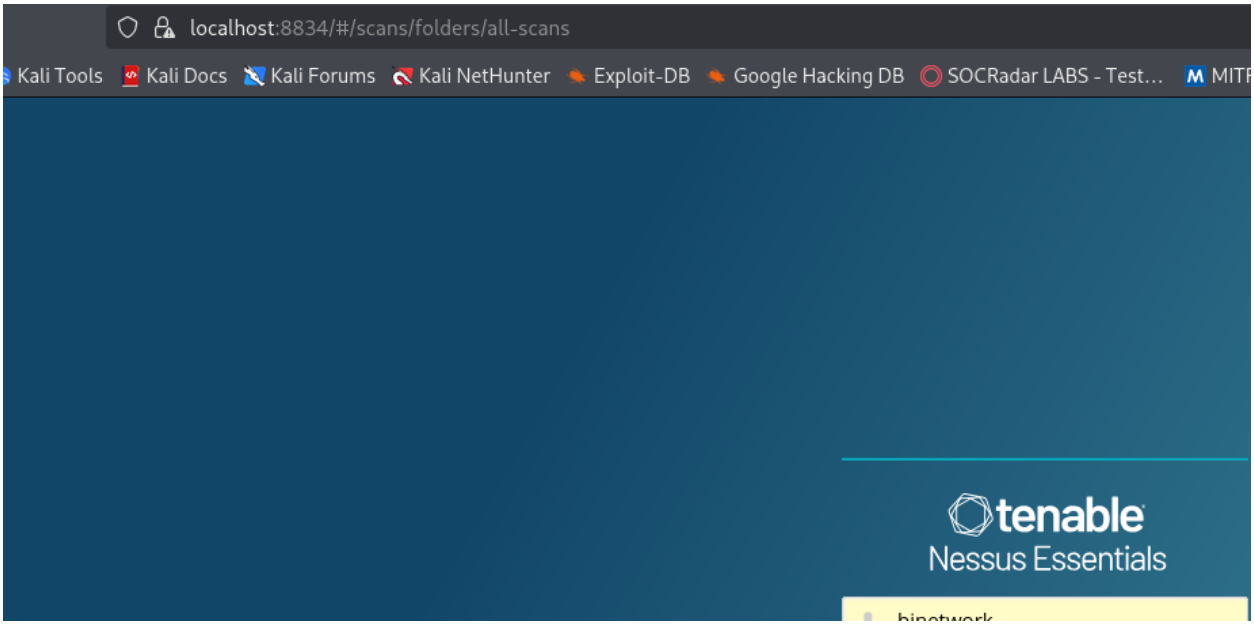
Wait time: 15-30 minutes for initial plugin compilation

bash

Monitor plugin compilation progress in terminal

sudo tail -f /opt/nessus/var/nessus/logs/nessusd.messages

Step 3: Log in to Nessus



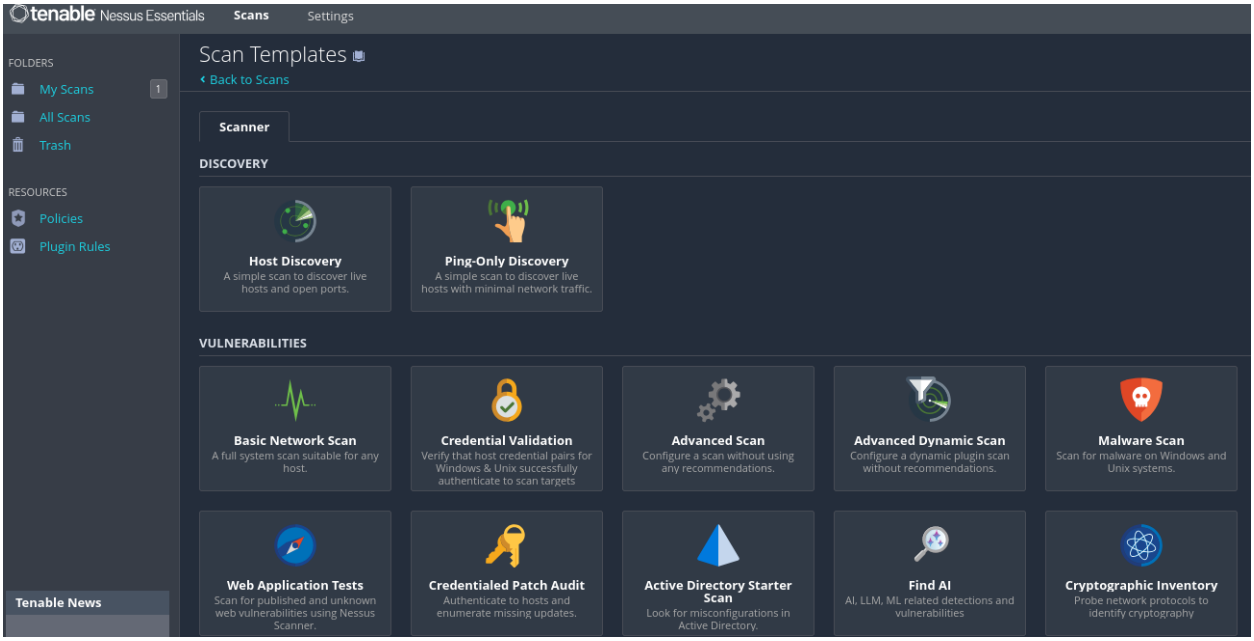
- Navigate to https://localhost:8834
- Enter your admin credentials
- You should see the main Nessus dashboard

Performing Vulnerability Scans

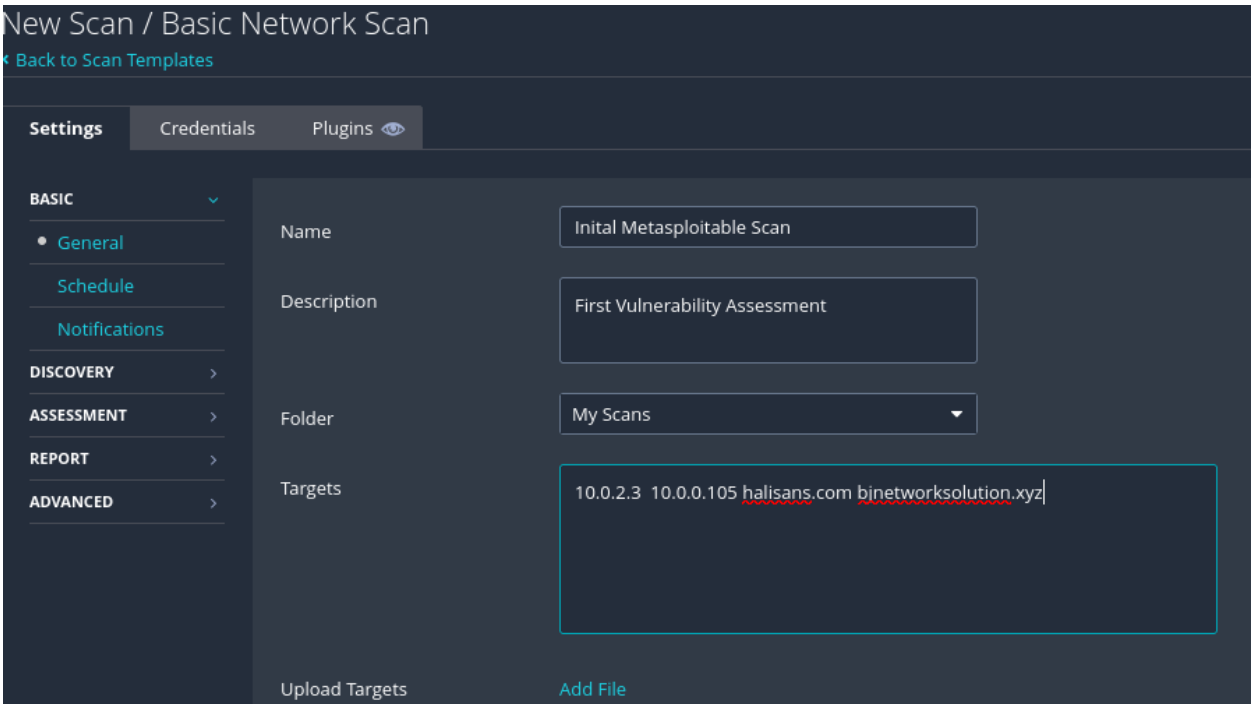
Scan Types Overview

Scan Type	Purpose	Credentials Required	Duration
Basic Network Scan	Quick vulnerability assessment	No	5-15 min
Advanced Scan	Customizable with specific plugins	Optional	10-30 min
Credentialed Scan	Deep system analysis	Yes	20-60 min
Web Application Scan	OWASP vulnerabilities	No	15-45 min
Malware Scan	Detect malicious processes	Yes	10-30 min

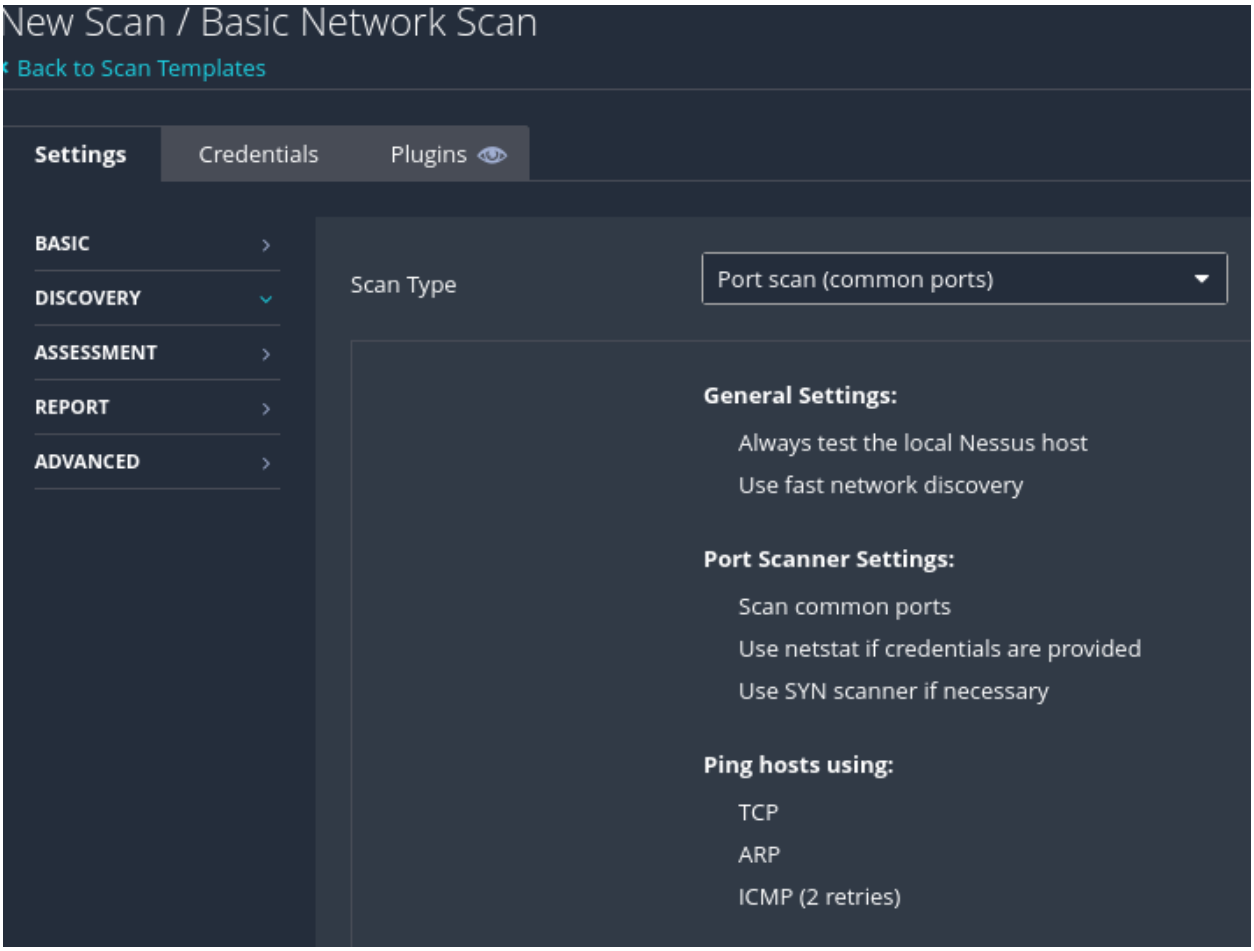
Step 1: Create a New Scan



1. Click the **"New Scan"** button
2. Select **"Basic Network Scan"** for beginners
3. Configure scan settings:
    - **Name**: "Initial Metasploitable Scan."
    - **Description**: "First vulnerability assessment."
    - **Folder**: My Scans
    - **Targets**: 192.168.56.101 (your target VM IP)



Step 2: Configure Scan Settings (Advanced)



Discovery Settings

Port Scanning:

- Port scan range: default (1-65535)

- Network discovery: Enabled

Assessment Settings

- General: Thorough tests

- Brute Force: Disabled (for initial scan)

- Web Applications: Enabled

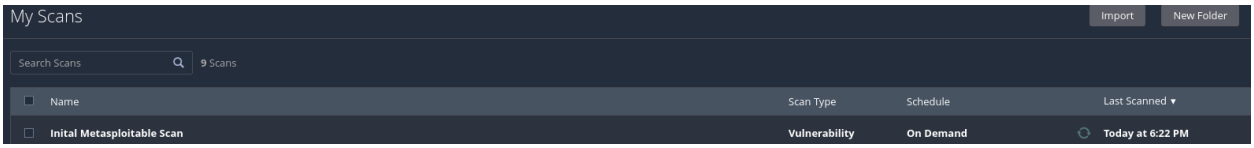
- Malware: Enabled

Report Settings

- Output: HTML, PDF, CSV

- Processing: Enabled

Step 3: Launch the Scan



1. Click **"Save"** to save scan configuration
2. Click **"Launch"** to start scanning
3. Monitor progress in real-time

bash

Find target VM IP address

On target machine, run:

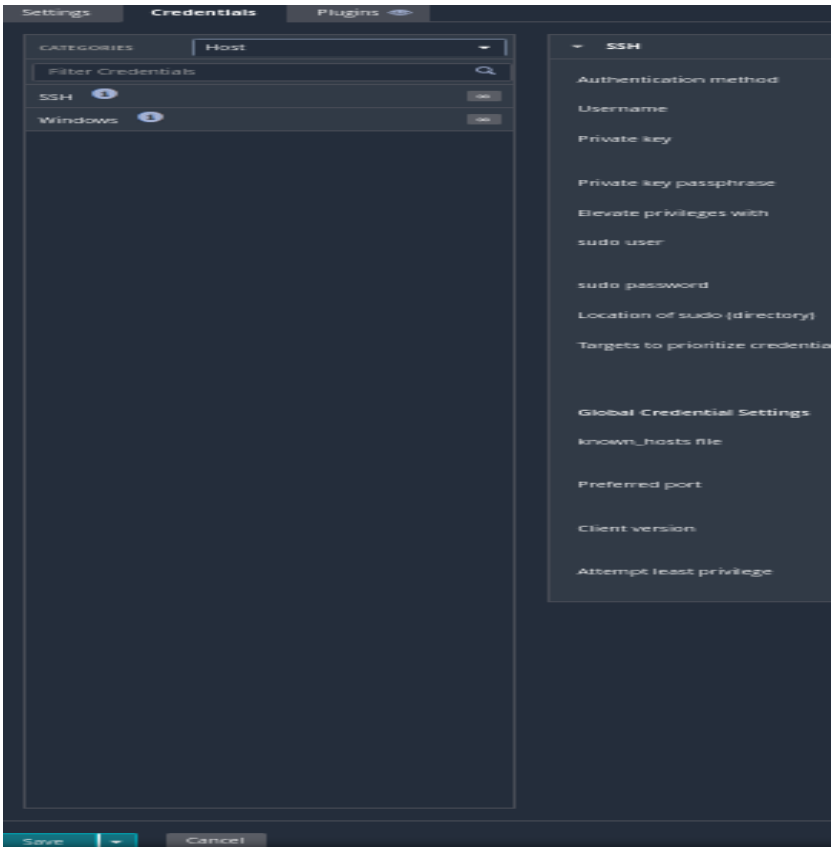
ifconfig

or

ip addr show

Step 4: Performing a Credentialed Scan

For deeper analysis, configure credentials:



-

1. Go to scan settings → **"Credentials"** tab
2. Select **"SSH"** for Linux targets
3. Add credentials:
    - **Username**: msfadmin
    - **Password**: msfadmin
    - **Privilege Escalation**: sudo
4. Save and launch scan

Analyzing Scan Results

Understanding the Dashboard

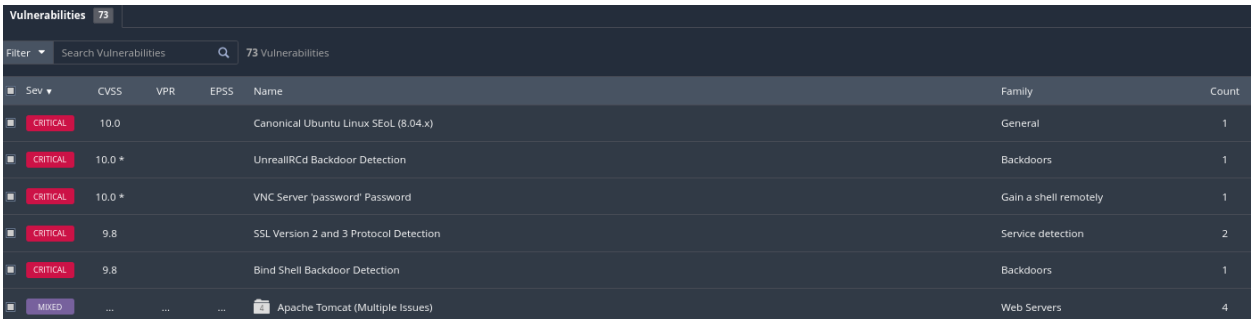
The results page displays:

- **Vulnerabilities by Severity**: Color-coded graph
- **Host Summary**: Number of hosts scanned
- **Vulnerability Count**: Total findings

Severity Ratings Explained

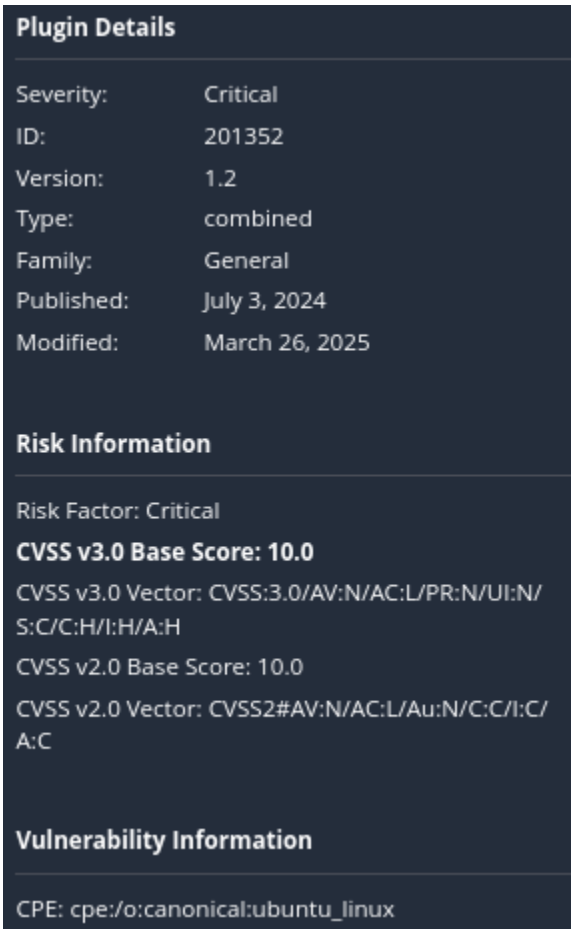
Severity	Color	CVSS Score	Priority	Action Required
Critical	Purple	9.0-10.0	Immediate	Patch within 24 hours
High	Red	7.0-8.9	Urgent	Patch within 1 week
Medium	Orange	4.0-6.9	Moderate	Patch within 1 month
Low	Yellow	0.1-3.9	Minor	Schedule maintenance
Info	Blue	0.0	FYI	No action needed

Step 1: Review Vulnerabilities by Host



1. Click on the target IP address
2. Review all detected vulnerabilities
3. Sort by **"Severity"** (Critical → Low)

Step 2: Examine Individual Vulnerabilities



For each vulnerability, Nessus provides:

Essential Information

- **CVE ID**: Common Vulnerabilities and Exposures identifier
- **Description**: What the vulnerability is
- **Solution**: How to fix it
- **See Also**: Reference links
- **Plugin Output**: Specific evidence found
- **CVSS v3 Score**: Industry-standard severity rating
- **Exploitability**: Ease of exploitation

Example Vulnerability Analysis

Vulnerability: Samba Remote Code Execution

CVE: CVE-2017-7494

CVSS Score: 9.8 (Critical)

Risk Factor: Critical

Description:

Samba versions 3.5.0 through 4.6.4 contain a remote code

An execution vulnerability that allows attackers to upload

a shared library to a writable share and execute arbitrary code.

Solution:

Upgrade to Samba version 4.6.4 or later

Exploit Available: Yes (Metasploit module exists)